UDC: 004.93: 60: 620 DOI: https://doi.org/10.15407/jai2021.01.085

INFORMATION TECHNOLOGIES AND THREATS IN CYBERPHYSICAL SYSTEMS FOR DISPLAYING INFORMATION IN UNDERGROUND METAL STRUCTURES WITH DEFECTS

R. Shuvar[1], A. Prodyvus[2], V. Yuzevych[3], I. Ogirko[4], O. Ogirko[5], R. Kovtko[6], R. Mysiuk[7]
[1,2,3,6,7]Ivan Franko National University of Lviv, Ukraine
1, University st., Lviv, 79000
[3]Karpenko Physico-Mechanical Institute of the National Academy of Sciences of Ukraine, Ukraine
5 Naukova st, Lviv, 79060
[4]Ukrainian Academy of Printing, Ukraine
19 Pod Holoskom st., Lviv, 79020
[5]Lviv State University of Internal Affairs, Ukraine
26, Horodotska st., Lviv, 79007

[1]http://orcid.org/0000-0001-6768-4695
[2]http://orcid.org/0000-0002-8701-2420
[3]http://orcid.org/0000-0001-5244-1850
[4]http://orcid.org/0000-0003-1651-3612
[5]http://orcid.org/0000-0002-4645-7933
[6]http://orcid.org/0000-0003-3324-2578
[7]http://orcid.org/0000-0002-7843-7646

Abstract. Software implementation of a system for data searching and acquisition received from measurement of underground metal structures with defects, is described. This system collects the data using sensors and sends them to the web service for further loading into the database. Information encryption algorithms for such a system are presented. The web service is suggested to use HTTPS, data transfer protocol with OAuth secret keys. The NoSQL Elasticsearch database can be encrypted and used as additional protection for the used data store. It should be noted that the search and selection of useful information concerns the electric currents and voltages obtained by measuring the sensors during non-destructive testing. The properties of cyber security and the requirements for information security are analyzed for the cyber-physical system. The types of attacks and threats in cyber-physical systems are described. The main elements of Security Metrics as a science for modeling system security are considered. The various important criteria of metals for defective underground metal structures are given. Defining the security version of a cyber-physical system helps to find changes from previous versions of the software and thus point to potential cyber security vulnerabilities. The importance of the corrosion detection stage for underground metal structures is noted. The next step is to verify the cyber-physical system for security problems using automated tools according to the criteria. The functional diagram for a secure connection in the specified system is given. Security checks of the cyber-physical system can be performed with unauthorized access to systems with error messages, codes, etc.

It was pointed out that the use of cryptographic techniques is advisable to preserve the confidentiality and integrity of the cyber-physical system.

Keywords: cyber-physical systems, attacks, cryptography, underground metal structures, defects, cracks, knowledge bases, big data, encryption of information.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ЗАГРОЗИ У КІБЕРФІЗИЧНИХ СИСТЕМАХ ДЛЯ ВІДОБРАЖЕННЯ ІНФОРМАЦІЇ У ПІДЗЕМНИХ МЕТАЛОКОНСТРУКЦІЯХ З ДЕФЕКТАМИ

Р.Я. Шувар[1], А.М. Продивус[2], В.М. Юзевич[3], І.В. Огірко[4], О.І. Огірко[5], Р.Т. Ковтко[6], Р.В. Мисюк[7]

[1,2,3,6,7]Ivan Львівський національний університет імені Івана Франка, Україна
вул. Університетська, 1, м.Львів, 79000
[3]Фізико-механічний інститут ім. Г.В. Карпенка НАН України, Україна
вул. Наукова, 5, м.Львів, 79060
[4]Українська академія друкарства, Україна
вул. Під Голоском, 19, м.Львів, 79020
[5]Львівський державний університет внутрішніх справ, Україна
вул. Городоцька, 26, м.Львів, 79007

[1]http://orcid.org/0000-0001-6768-4695
[2]http://orcid.org/0000-0002-8701-2420
[3]http://orcid.org/0000-0001-5244-1850
[4]http://orcid.org/0000-0003-1651-3612
[5]http://orcid.org/0000-0002-4645-7933
[6]http://orcid.org/0000-0003-3324-2578
[7]http://orcid.org/0000-0002-7843-7646

Анотація. Розглянуто кіберфізичні системи (КФС) і приклад їх використання для системи пошуку та відбору інформації з вимірювальних пристроїв у підземних металоконструкціях з дефектами. Інформація передається від сенсорів до вебсервісу з подальшим записом у базі даних. Представлено принципи формування алгоритмів шифрування інформації для такої системи. У вебсервісі запропоновано використовувати протокол передачі даних з OAuth (HTTPS). Відповідна нереляційна база даних (ElasticSearch) може шифруватися і створювати додатковий захист для сховища даних. Відбір експериментальних даних запропоновано отримувати, використовуючи вимірювач поляризаційного потенціалу (ВПП) у комплексі з безконтактним вимірювачем струму (БВС). Варто зазначити, що пошук та відбір корисної інформації стосується електричних струмів та напруг, отриманих вимірювальними сенсорами в умовах неруйнівного контролю. Проаналізовано властивості кібербезпеки для кіберфізичної системи та вимоги щодо засобів захисту інформації у складі кіберфізичної системи. Описано типи атак та загроз у кіберфізичних системах. Розглянуто елементи безпекометрії як науки для моделювання безпеки КФС. Для підземних металоконструкцій з корозійними дефектами типу тріщин подано інформацію про такі важливі критерії як міцність і пластичність.

Визначення версії безпеки КФС допомагає знайти зміни щодо попередніх версій програмного забезпечення і, таким чином, вказати на потенційні вразливості у сфері кібербезпеки. Відзначено важливість етапу виявлення корозійних дефектів для підземних металоконструкцій. Подальший етап пов'язаний з перевіркою КФС на наявність проблем безпеки за допомогою автоматизованих засобів, відповідно до критеріальних умов. Функціональна схема додається для опису безпечного з'єднання у зазначеній системі. Перевірку безпеки КФС можна проводити у вигляді несанкціонованого доступу до системи з повідомленнями про помилки, коди тощо.

Відзначено, що для збереження конфіденційності та захисту цілісності інформації КФС доцільно використовувати криптографічні методи.

Ключові слова: кіберфізичні системи, атаки, криптографія, підземні металоконструкції, дефекти, тріщини, великі дані, шифрування інформації.

Вступ

Захист інформації є актуальним, оскільки комп'ютерні технології (КТ) використовуються у більшості сфер нашого життя, а безпека для них важлива. Кіберфізичні системи (КФС) пов'язані зі

сферою діяльності, яка забезпечує елементи взаємодії між реальним світом та інформаційними системами. Основною метою кіберфізичних систем є контроль поведінки фізичних об'єктів, частиною яких вони є [1]. КФС не є традиційними системами у режимі реального часу, вони надають додаткові властивості класичним системам. Їх кібер- і фізичні компоненти інтегровані для навчання та адаптації, самоорганізації та продуктивності.

Прикладом КФС є система пошуку та відбору інформації про дефекти типу тріщин у підземних металоконструкціях (ПМК). Дефекти на поверхні ПМК виникають досить часто у зв'язку з механічними навантаженнями та специфікою ґрунтового покриву [2]. Для зберігання даних про різного типу тріщини потрібно використовувати базу знань. Розробка вебсервісів для розв'язання різних задач у сфері функціонування КФС стає в останній час популярним напрямком діяльності. Зокрема, з метою забезпечення безпеки отримання даних розробляють вебсервіси і використовують їх для розв'язання різноманітних популярних задач технологічного спрямування.

Огляд літератури

Зазвичай важливою технологічною проблемою матеріалознавства є розроблення методик забезпечення надійної взаємодії систем управління з фізичними системами [1]. Інформаційні системи з кожним днем стають усе складнішими, і тому найменший витік інформації може стати фатальним [3]. У зв'язку з цим, сучасні дослідження спрямовані на створення систем, які б змогли збалансувати поєднання фізичних і обчислювальних елементів [1]. У цьому контексті доцільно використовувати кіберфізичні системи (КФС) [1, 3]. Загалом, відомо багато методів забезпечення безпеки КФС [1]. Проте, вони спрямовані більше на захист інформації, а не фізичних систем [3]. На практиці ці методи можуть бути неефективні через людські помилки, неточності програмного забезпечення, збої у налаштуванні пристроїв [1]. Наслідком цього можуть бути успішні атаки зловмисників на КФС [3]. Захист даних за допомогою шифрування – одне з можливих розв'язань проблеми безпеки [1, 3]. Зашифрований текст стає доступним тільки для того, хто знає секретний ключ [3]. Такого типу питаннями займаються спеціалісти криптографії [3]. Все ще немає чітких вимог щодо криптографічного захисту інформації, тому в даній статті будуть сформульовані властивості, якими має володіти КФС для ПМК з дефектами, щоб бути надійною [3].

Мета роботи

Метою роботи є узагальнення типів атак та загроз у кіберфізичних системах, а також формулювання криптографічних вимог до КФС для ПМК з дефектами. Основним завданням кіберфізичних систем є контроль поведінки фізичного об'єкта, частиною якого вони є, а також можливіть зміни поведінки системи за необхідності. Кіберфізичні системи часто поєднують великий обсяг кібернетичних, телекомунікаційних, обчислювальних засобів, засобів штучного інтелекту, автоматики, вимірювання й управління, а також захисту інформації [1].

Методи дослідження

Для розв'язання задач створення інформаційних технологій (ІТ) відбору і обробки даних від металоооб'єктів в умовах ризику та невизначеності на основі розробленої концепції функціонування КФС використано елементи: теорії системного аналізу, теорії управління в ієрархічних системах, теорії інформації, теорії сигналів, методи стандартизації та сертифікації, а також методи захисту інформації.

Виклад основного матеріалу

Кіберфізична система передбачає інтеграцію сучасних обчислювальних ресурсів у фізичні процеси. У такій системі (КФС) сенсори, обладнання та ІТ-системи в технології ПМК з'єднані вздовж всього ланцюжка створення вартості, що виходить за межі одного підприємства. Ці системи в технології ПМК взаємодіють одна з одною

за допомогою стандартних інтернет-протоколів для прогнозування, самонастроювання і адаптації до змін. Кіберфізичні системи відносяться до сфери четвертої промислової революції [1]. Можна перелічити ключові технологічні тенденції, які лежать в основі КФС для ПМК з дефектами. Ізольовано вони вже використовуються в різних сферах, але, будучи інтегрованими в єдине ціле, вони змінюють існуючі відносини між людиною та машиною. Незалежно від сфери застосування КФС, характерні такі основні особливості [3]:

– залежність від середовища виконання. КФС досить тісно пов’язані з середовищем, в якому вони працюють (фізичні об’єкти). Будь-яка зміна в поведінці середовища призводить до зміни поведінки КФС;
– чітко визначені можливості. КФС, для яких, як правило, властиві декілька компонентів, що мають різні характеристики. Сенсори, які вбудовані в фізичні пристрої з метою моніторингу, мають обмежені можливості, а програмні засоби, що допомагають керувати цими сенсорами, є відносно потужнішими. Для КФС, на відміну від традиційних автономних вбудованих систем, потрібен мережевий зв'язок між компонентами для того, щоб вони надавали свої послуги. Технології великих даних дозволять використовувати у цьому плані різні симулятори в режимі реального часу.

Створити платформи для спільної роботи й обміну даними між територіально-розподіленими партнерами дозволяють хмарні технології. Інтернет речей в технології ПМК призводить до того, що показники сенсорів зазвичай потрапляють в централізовану систему керування виробничим процесом і вже на цьому рівні користувачі приймають рішення.

Важливою для КФС, які стосуються ПМК з дефектами, є інформаційна безпека. При цьому багато компаній використовують системи, що ґрунтуються на пріоритетних технологіях виробництва. Але в міру розширення зв'язків з партнерами (використання відкритих стандартів і протоколів), різко зростають ризики у контексті інформаційної безпеки.

Роботу кіберфізичних систем можна розділити на три етапи [1]:

1.Моніторинг – найголовніший етап у роботі КФС, який полягає в спостереженні за змінами середовища, в якому працює КФС. Його також використовують для отримання відгуків на будь-які дії, які відбувалися у минулому з КФС. Це потрібно для того, щоб уникнути збоїв системи у майбутньому.

2.Опрацювання даних, яке стосується аналізу даних, зібраних у ході моніторингу для того, щоб дізнатися, чи фізичний процес відповідає попередньо визначеним критеріям. Коли критерії не задоволено, коригувальні дії дозволяють системі переходити до інших критеріїв. Для ПМТ з дефектами важливі критерії міцності та пластичності металу, а також критерії протикорозійного захисту [5, 6].

3.Виконання функцій. На цьому етапі виконуються дії, визначені на етапі опрацювання даних. При цьому поведінка КФС може бути змінена повністю.

Будь-яка КФС може перебувати в одному з трьох можливих режимів: пасивний, пасивно-активний та активний [1]. Доповнена реальність – відповідна технологія перебуває на початковій стадії свого розвитку, але в майбутньому допоможе прискорити прийняття рішень.

КФС охоплюють цілі галузі з різною швидкістю і в різних напрямках. Галузі із широкою продуктовою лінійкою, такі як автомобільна, продукти харчування, виграють від гнучкості кіберфізичних систем і зростання продуктивності. Галузі, що вимагають високої якості, такі як електроніка, виграють від використання великих даних і аналітики, безперервного поліпшення якості та функціональності продукції. В цілому, більш гнучкі, швидкі й ефективні способи отримання якісних товарів за зниженими цінами призводять до зростання економіки, кваліфікованих робочих місць і, в кінцевому підсумку, змінюють конкурентоспроможність компаній і регіонів. Такі системи в технології ПМК [2, 5] покликані підвищити

рівень взаємодії людини з фізичним світом, подібно до того, як інтернет підвищив рівень взаємодії між людьми. Основною проблемою у цьому контексті є така: як інтегрувати різнотипні компоненти (методи і засоби вимірювання, керування, захисту інформації) та забезпечити їх якісну ефективну взаємодію, що дозволило б збирати максимум необхідних даних, виокремлювати з них корисну, потрібну людині інформацію, а також, можливо, впливати на фізичний світ, скажімо, у виробничій сфері.

Найпоширенішими сферами діяльності кіберзлочинців на даний час є: вплив на функціонування окремих вузлів чи сегментів мережі, пошкодження функціонування інформаційних систем і заволодіння особистою інформацією. користувача за допомогою спеціальних програмних скриптів і програмних засобів, що потрапляють у комп'ютерну систему в процесі інтернет-серфінгу (Adware) [3, 8]. Тому постає практична проблема компенсації пошкодження мережевого трафіку та структури і вмісту пакетів даних комп'ютерних мереж у процесі скоєння кіберзлочинів.

Розв'язання практичної проблеми у цьому плані вбачаємо в досягненні мети наукової роботи: забезпечити підвищення рівня функціонування комп'ютерних мереж передачі даних за рахунок інформаційних технологій обробки трафіку для боротьби з кіберзлочинністю. Боротьба з кіберзлочинністю передбачає використання методології шифрування (рис. 1) [3] SSL (Secure Sockets Layer) та TSL (Transport Layer Security).

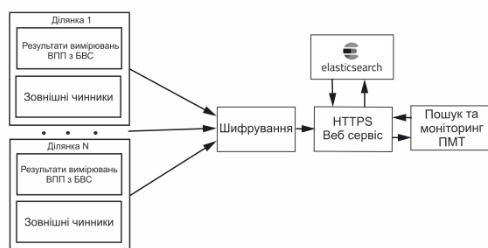


Рис. 1. Структурна схема безпеки системи пошуку та відбору інформації про дефекти (тріщини)

Кіберфізичну систему можна застосувати для системи пошуку та відбору інформації про дефекти типу тріщин (рис.1). Досліджуваних ділянок ПМК з дефектами типу тріщин може бути декілька. Відповідно і даних, які надсилаються до створеного вебсервісу для пошуку та відбору цих даних, є велика кількість [5, 6, 9]. Опрацювання такої великої кількості даних потребує перевірки їх правильності та реальності. Одним із найвідоміших варіантів вебшифрування є HTTPS (Hypertext Transfer Protocol Secure), протокол передачі даних, який використовує криптографічні протоколи SSL (Secure Sockets Layer) та TSL (Transport Layer Security). Крім цього, для більшої безпеки використовують різноманітні додаткові елементи захисту, наприклад OAuth. Підтримка таких рішень забезпечить безпеку отримання даних. Крім цього, сформовану базу знань на основі нереляційної бази даних ElasticSearch можна шифрувати [4]. Безпосередньо перевірка правильності різних секретних ключів відбувається у вебсервісі перед додавання цих даних до бази знань. Такий підхід дозволить забезпечити безпеку відповідного вебсервісу. Оскільки відбір даних може відбуватися з вимірювача поляризаційного потенціалу (ВПП) у комплексі з безконтактним вимірювачем струму (БВС) [5, 6], то комплексна перевірка структури та правильності інформації у базі знань є обов'язковою, щоб не допустити в системі загроз від різного типу атак.

Сформульована мета дає змогу скласти можливий перелік завдань для розв'язання поставленої практичної проблеми. Структурно можна виділити три головні завдання цієї праці:

- розробка ІТ уникнення перевантаження трафіку для запобігання відмовам в обслуговуванні (DoS) на основі механізмів гарантованого рівня якості обслуговування (OoS);
- розробка ІТ підвищення швидкості функціонування запитів для протидії кібератакам на інформаційні системи; розробка ІТ перехоплення та блокування трафіку на основі структурного та

сигнатурного аналізу для блокування загроз AdWare.

Забезпечення гарантованого рівня якості обслуговування (QoS) під час передачі мережевих даних, відповідно до специфіки сучасних інформаційних потоків в умовах інтенсивного зростання кількості користувачів Інтернету, збільшення обсягу трафіку та підвищення імовірності зловмисних дій кіберзлочинців, що спричинюють відмову в обслуговуванні (DoS), має пріоритетне значення для сучасних мультисервісних інформаційних систем (ІС). ІС зазвичай є складними багатопараметричними і слабко-детермінованими динамічними системами [4]. У багатьох випадках інформація про характеристики та параметри таких систем, їх динаміку та зовнішні впливи недостатня або невідома. Як наслідок, постає задача параметричної ідентифікації моделей процесів передачі інформаційних потоків. Інформаційна гарантоздатність – це комплексна властивість системи надавати необхідні послуги, яким можна виправдано довіряти [7].

Гарантоздатність включає:

- безвідмовність – властивість надавати необхідні послуги впродовж заданого часу;
- готовність – властивість доступності ресурсів для надання необхідних послуг;
- обслуговуваність – властивість пристосовуватись до модифікацій та обслуговування;
- живучість – властивість мінімізувати зниження працездатності та зберігати в прийнятних межах обсяг та якість надаваних послуг у разі відмов, обумовлених зовнішніми впливами;
- функціональна безпека – властивість виключати або мінімізувати шкідливі наслідки у разі відмов для користувачів або інших систем;
- цілісність – властивість виключати непередбачені зміни даних та наданих послуг;
- конфіденційність – властивість перешкоджати неавторизованому доступу до інформації обмеженого доступу;
- вірогідність – властивість правильно оцінювати коректність наданих послуг, визначати ступінь довіри до послуги [6].

Безпекометрія, це:

- наука про моделювання безпеки;
- наука, яка вивчає числові закономірності ефективного забезпечення безпеки у соціальних, біологічних та технічних системах, котрі реалізуються за допомогою відповідних відносин у сфері безпеки;
- галузь науки, що здійснює свою мету на базі творчого статистичного осмислення та концептуального моделювання, засобів керування, синергетики, біології, генетики, права, стратегії, соціології, антропології та багатьох інших наук.

Безпекометрія є науковим напрямком моделювання безпеки; суспільна міждисциплінарна сфера діяльності, яка чисельно досліджує загальні та специфічні об'єктивні закономірності організації та функціонування систем безпеки різного класу і виробляє на підставі їх пізнання загальні теоретичні положення, які спрямовані на підвищення ефективності їх функціонування [3].

Безпекометрія допомагає впорядкувати на основі деяких аспектів діяльності показники безпеки системи або підприємства з урахуванням параметрів, які піддаються кількісному вимірюванню. Для певних об'єктів, для яких безпека є змістовним поняттям, існує декілька ідентифікованих ознак, які в сукупності характеризують безпеку цього об'єкта [3 – 8]. Інформаційно-комунікаційні технології безпекометрії виробництва — сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою відбору, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів [1, 3]. Інформаційна технологія безпекометрії виробництва — цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечать високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації, незалежно від місця їх розташування. Інформаційна

технологія безпекометрії виробництва – це сукупність методів, виробничих процесів та програмно-технічних засобів, об'єднаних у технологічний ланцюжок, що забезпечує виконання інформаційних процесів з метою підвищення їхньої надійності та оперативності й зниження трудомісткості ходу використання інформаційного ресурсу.

Важливо відзначити механізми, які реалізуються сукупністю технічних, програмних та інших засобів, що забезпечують збереження та автоматичне відновлення за обмежений час працездатного інформаційно-технічного стану під час виникнення відмов. Комплексна властивість програмно-технічних комплексів критичного призначення техніки поєднує аспекти надійності, функціональної та інформаційної безпеки та забезпечує здатність КФС надавати необхідні послуги, яким можна оправдано довіряти.

Єдиний підхід до ІТ відбору даних від об'єктів обґрунтовує системні критерії: безпечного функціонування технологічних та природних систем; функціональної та інформаційної безпеки ІТ. Наука і практика зацікавлені у такому підході, оскільки він системний і синтезує кілька наукових напрямків. Тому актуальним є питання розроблення методологічних засад та засобів створення ІТ відбору і обробки різнорідних даних від систем у контексті безпечного функціонування КФС. Методи і засоби оцінювання технічного стану об'єктів в умовах невизначеності, які узгоджені з основними методами неруйнівного контролю (НК) і становлять основу для створення підходів, методологій та методик, спрямованих на фізико-механічних властивостей металоконструкцій та прогнозування їх залишкового ресурсу, повинні ґрунтуватись на відборі сигналів від власних фізичних полів металоконструкцій, оскільки це дозволяє отримати фактичну інформацію про технічний стан об'єкта. Методи і засоби ІТ відбору даних про стан техногенних систем, в міру закладених критеріїв ефективності реєстрації сигналів від об'єктів, дозволяють з відповідною точністю визначати параметри їх стану, оцінювати роботоздатність, якість, прогнозувати залишковий ресурс і спрямовані на забезпечення безпеки експлуатації в умовах дії зовнішніх факторів.

Оскільки ІТ є основним інструментарієм розв'язання прикладних задач у предметних сферах, то єдиний підхід до створення методів і засобів відбору й обробки даних від техногенних систем обґрунтовує системні критерії безпеки: "міцність – ресурс" об'єктів та "захищеність – гарантоздатність" автоматизованих систем за дії факторів впливу в умовах експлуатації (навантаження, агресивного середовища (водню, сірководню), водного середовища). Розроблення та реалізація концепції створення ІТ відбору різнорідних даних від техногенних систем у контексті забезпечення стратегічної безпеки структури «об'єкт – ІТ» є актуальною проблемою наукових досліджень. Її розв'язання є доцільним, оскільки сприяє розвитку ІТ досліджень властивостей матеріалів у контексті стратегічної безпеки об'єктів, завдяки:

1) вдосконаленню методик створення нових методів та засобів відбору й обробки інформації про фактичний стан техногенних систем на рівні процесів відбору параметрів сигналів для мінімізації ресурсного ризику «дефект – руйнування – загроза – збитки»;
2) вдосконаленню та створенню методів і засобів забезпечення безпеки автоматизованих систем для мінімізації інформаційного ризику у структурі функціонального ризику.

Новизна отриманих результатів полягає в тому, що запропоновано інформаційну технологію для задач керування безпекою КФС на основі моделі стратегічної безпеки структури, інфраструктури, інформатизації, системної концепції створення методів і засобів відбору даних та оцінювання параметрів стану, яка методологічно трансформується у відповідні предметні сфери і дозволяє цілісно розв'язувати проблему забезпе-

чення безпеки об'єктів за впливу множини факторів.

Запропоновано в межах КФС: підхід до відбору різнорідних даних від об'єктів на основі процедур та методології вимірювання фізичних величин, які комплексно дозволяють реалізувати інформаційні технології для прикладних задач контролю, діагностування, розпізнавання, прогнозування стану ПМК; підхід до методики виконання вимірювань параметрів ПМК, що дозволяє застосовувати ІТ для контролю стану об'єктів в умовах ризику. Метою також є визначення ресурсу ПМК в межах обсягу фізичних величин та послуг, які у цьому випадку задіяні. Цей етап також призначений для виявлення вразливих місць. Визначення версії безпеки КФС допомагає знайти зміни з попередніх версіях програмного забезпечення і, таким чином, вказати на потенційні вразливості. Після етапу виявлення корозійних дефектів цей етап сприяє перевірці КФС на наявність відомих проблем безпеки за допомогою автоматизованих засобів, відповідно до критеріальних умов. Перевірка безпеки КФС може проводитися у вигляді несанкціонованого доступу до системи з повідомленнями про помилки, коди тощо. За допомогою оцінювання параметрів безпеки КФС тестувальники прагнуть отримати широке уявлення про систему, але без подробиць про її внутрішню функціональність.

Кожна функція КФС має власний специфічний набір заходів безпеки. Багато кіберфізичних додатків є системами щоденного використання, користувачі яких, як правило, недостатньо обізнані з технікою. Це, зокрема, системи медичного моніторингу, смарт інфраструктури (Smart Infrastructure) тощо.

Тому аспекти безпеки для КФС повинні бути зручними у використанні. Для того, щоб уникнути атаки на систему, необхідно дотримуватись таких вимог безпеки як конфіденційність. Під конфіденційністю розуміють здатність приховувати дані [1, 3]. Це, зазвичай, досягається за допомогою криптосистем.

Криптосистема – це математична функція, яка перетворює вхідне повідомлення на зашифрований текст [3]. Зашифрований текст може бути перетворений у початковий стан тільки за наявності інверсної функції. Процеси шифрування й розшифрування можуть відбуватися тільки за допомогою криптографічного ключа. Розшифрувати повідомлення достатньо складно, а то й практично неможливо, не знаючи точного значення ключа. Існують два типи криптографічних систем, які можна використовувати для забезпечення конфіденційності: симетричні та асиметричні криптосистеми [3].

З вище наведених даних можна зробити висновок, що для збереження конфіденційності та захисту цілісності інформації основною вимогою є використання криптографічних методів. Процес криптографічного закриття даних може здійснюватись як програмно, так і апаратно [3]. Апаратна реалізація відрізняється суттєво більшою вартістю, проте має і переваги: високу продуктивність, простоту, захищеність. Програмна реалізація більш практична і забезпечує суттєву гнучкість у використанні. Незалежно від способу реалізації, для сучасних криптографічних систем захисту інформації визначено вимоги [1, 3]. Знання алгоритму шифрування не повинно знижувати криптостійкість шифру. Вибір криптографічної технології має задовольняти вимоги надійності [1, 3]. Зашифроване повідомлення повинно бути прочитаним тільки за наявності ключа [3]. Шифр повинен бути стійким, навіть коли зловмиснику відома достатня кількість вхідних даних і відповідних їм зашифрованих даних. Незначна зміна ключа або вихідного повідомлення повинна приводити до істотної зміни вигляду зашифрованого тексту. Структурні елементи алгоритму шифрування повинні бути незмінними [3]. Довжина шифрованого повідомлення повинна дорівнювати довжині вихідного повідомлення. Додаткові біти, які вводяться в повідомлення, у процесі шифрування

повинні бути повністю і надійно приховані в шифрованому повідомленні. Будь-який ключ із множини можливих повинен забезпечувати однакову криптостійкість. Не повинно бути простих і легковстановлюваних залежностей між ключами, які послідовно використовуються в процесі шифрування.

Висновки

У роботі наведено характеристики кіберфізичних систем (КФС), які стосуються підземних металоконструкцій (ПМК) з дефектами, а саме: залежність від середовища функціонування; чітко визначено можливості функціонування та мережевість. Необхідно враховувати такі різновиди атак, як: обманні атаки, DoS-атаки, прямі атаки на КФС. Розглянуто варіанти безпекометрії стосовно КФС для ПМК з дефектами. Розглянуто особливості безпеки для КФС ПМК та основні загрози у сфері кіберфізичної безпеки стосовно цих систем. Сформульовано основні вимоги до КФС з урахуванням алгоритмів шифрування інформації.

Для ПМК з корозійними дефектами типу тріщин приведено інформацію про необхідність врахування критеріїв міцності та пластичності, з допомогою яких контролюємо ресурс конструкцій.

Перспективними є розробки КФС для конструкцій авіаційно-космічного призначення із стільниковими наповнювачами.

References

1. Melnyk A. (2014) Cyber-physical systems: the problems of creation and directions of development. Lviv: Lviv Polytechnic Publishing House. – P. 154–161.
2. Yuzevych V., Pavlenchyk N., Zaiats O., Heorhiadi N., Lakiza V. (2020) Qualimetric Analysis of Pipelines with Corrosion Surfaces in the Monitoring System of Oil and Gas Enterprises / // International Journal of Recent Technology and Engineering (IJRTE), Vol. 9, No. 1. P. 1145–1150. DOI:10.35940/ijrte A1341.059120.
3. Barychev S., Serov R. (2002) Osnovy sovremennoi cryptographii. – Moscow: Horiachaia lynyia – Telekom. – P. 175.
4. Shaik S., Naga N., Rao M. A Review of Elastic Search: Performance Metrics and challenges (2017). International Journal on Recent and Innovation Trends in Computing and Communication:. P. 222-229. URL:https://www.academia.edu/36852634/A_Review_of_Elastic_Search_Performance_Metrics_and_challenges.
5. Yuzevych V., Pavlenchyk A., Lozovan V., Mykhalitska N. & Bets M. (2020). Diagnostics of Temperature Regime of Technological Environments of Underground Pipelines in the Monitoring System of Oil and Gas Enterprises for Providing of Safe Exploitation. International Journal of Recent Technology and Engineering (IJRTE), 9 (1), P. 1301–1307. http://doi.org/10.5281/zenodo.3841334.
6. Yuzevych V., Horbonos F., Rogalskyi R., Yemchenko I. & Yasinskyi M. (2020) Determination of the Place Depressurization of Underground Pipelines in the Monitoring of Oil and Gas Enterprises. International Journal of Recent Technology and Engineering (IJRTE), 9(1), P. 2274–2281. http://doi.org/10.5281/zenodo.3841287.
7. B. Mudla, T. Yefimova, R. (2010) Dependability as a fundamental generalizing and integrating approach. P. 148-165. URL:http://dspace.nbuv.gov.ua/bitstream/handle/123456789/51596/19-Mudla.pdf?sequence=1.
8. R. Rajkumar, I. Lee, L. Sha, J. Stankovic Cyber-physical systems: the next computing revolution (2010) Proceedings of the 47th Design Automation Conference, DAC 2010, Anaheim, California, USA. https://doi.org/10.1145/1837274.1837461.
9. Sirajum Munir, Hao-Tsung Yang, Shan Lin, S. M. Shahriar Nirjon, Chen Lin, Enamul Hoque, John A. Stankovic, and Kamin Whitehouse. 2019. Reliable Communication and Latency Bound Generation in Wireless Cyber Physical System. ACM Transactions on Cyber-Physical Systems 1, 1 (July 2019), 25 pages. https://doi.org/10.1145/3354917.

Література

1. Мельник А.О. (2014) Кіберфізичні системи: проблеми створення та напрями розвитку. Львів: Видавництво Львівської політехніки. – С. 154–161.
2. Yuzevych V., Pavlenchyk N., Zaiats O., Heorhiadi N., Lakiza V. (2020) Qualimetric Analysis of Pipelines with Corrosion Surfaces in the Monitoring System of Oil and Gas Enterprises // International Journal of Recent Technology and Engineering (IJRTE), Vol. 9, No. 1. P. 1145–1150. DOI:10.35940/ijrte.A1341.059120.
3. Баричев С.Г., Серов Р.Е. (2002) Основы современной криптографии. – М.: Горячая линия – Телеком. – С. 175.
4. Shaik S., Naga N., Rao M. A Review of Elastic Search: Performance Metrics and challenges (2017). International Journal on Recent and Innovation Trends in Computing and Communication. С. 222-229.

URL:https://www.academia.edu/36852634/A_Review_of_Elastic_Search_Performance_Metrics_and_challeges.

5. Yuzevych V., Pavlenchyk A., Lozovan V., Mykhalitska N., Bets M. (2020) Diagnostics of Temperature Regime of Technological Environments of Underground Pipelines in the Monitoring System of Oil and Gas Enterprises for Providing of Safe Exploitation. International Journal of Recent Technology and Engineering (IJRTE), 9 (1), P. 1301–1307. http://doi.org/10.5281/zenodo.3841334.
6. Yuzevych V., Horbonos F., Rogalskyi R., Yemchenko I., Yasinskyi M. (2020) Determination of the Place Depressurization of Underground Pipelines in the Monitoring of Oil and Gas Enterprises. International Journal of Recent Technology and Engineering (IJRTE), 9(1), P. 2274–2281. http://doi.org/10.5281/zenodo.3841287.
7. Мудла Б.Г, Єфімова Т.І, Рудько Р.М. (2010) Гарантоздатність як фундаментальний узагальнюючий та інтегруючий підхід. Математичні машини і системи. С. 148-165. URL:http://dspace.nbuv.gov.ua/bitstream/handle/123456789/51596/19-Mudla. pdf?sequence=1.
8. R. Rajkumar, I. Lee, L. Sha, J. Stankovic Cyber-physical systems: the next computing revolution (2010) Proceedings of the 47th Design Automation Conference, DAC 2010, Anaheim, California, USA. https://doi.org/10.1145/1837274.1837461.
9. Sirajum Munir, Hao-Tsung Yang, Shan Lin, S. M. Shahriar Nirjon, Chen Lin, Enamul Hoque, John A. Stankovic, and Kamin Whitehouse. 2019. Reliable Communication and Latency Bound Generation in Wireless Cyber Physical System. ACM Transactions on Cyber-Physical Systems 1, 1 (July 2019), 25 pages. https://doi.org/10.1145/3354917.

Received 20.04.21
Accepted 25.05.21